

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA)
) Criminal No. 04-10317-RCL
 v.)
ANDREW LEWIS)

GOVERNMENT'S OPPOSITION TO DEFENDANT'S
MOTION TO SUPPRESS STATEMENTS AND PHYSICAL EVIDENCE

The United States of America, by and through undersigned counsel, hereby opposes the defendant's Motion to Suppress Statements and Physical Evidence, referred to here as the defendant's Motion. By the Motion, the defendant seeks to suppress (1) various images found on three computers owned or used by the defendant, and (2) various statements the defendant made to law enforcement officers during the course of a year long investigation. As discussed below, the defendant's statements were voluntary, and the searches were either supported by consent or warrant. Accordingly, the defendant's motion is without merit and should be denied.

Relevant Facts

A. The case starts with the Salem Maritime National Historic Site.

This case has its origin in events that took place in the basement of a building at the Salem Maritime National Historic Site ("SAMA") in Salem, Massachusetts. The SAMA is a federally owned site consisting of approximately five buildings. The National Park Service ("NPS") oversees the day to day operations

of the SAMA and employs approximately 35-40 employees there in a variety of positions, including administrative, security, maintenance and volunteer. For security and general police-like purposes, the NPS as of 2003 employed a total of four Law Enforcement Park Rangers ("Park Rangers"); the defendant was one of these four Park Rangers.

One of the buildings at the SAMA is the multi-story old Customs House building, located at 178 Derby Street.¹ Much of the building is open to the public and tours are given on a regular basis. There is a basement to the building which, while not open to the public, serves a variety of functions for SAMA employees.

The basement area is divided roughly into thirds; a blueprint layout of the basement is attached as Exhibit One. As one descends the stairs and enters the basement --through the doorway marked "Entrance" on the blueprint, there is a door leading to a room which serves as the employees' lunch/break room. At the back wall of the lunch/break room is another door which leads to a room reserved for the four Park Rangers. The middle area of the basement consists of a resource/library area containing pertinent books, periodicals, rules, regulations, etc. Finally, if one goes to the right, through the area where boilers

¹This is the actual address of the building but the mailing address for this and an adjacent building is 174 Derby Street.

are indicated, there is an entrance to a storage room, marked "Computer Storage" on the blueprint. Aside from the room reserved for the Park Rangers, all SAMA employees had access to all areas of the basement, including the storage area.

B. In January of 2003, the defendant placed his personal computer in the storage area alongside several old NPS computers.

The defendant and many other NPS employees at the SAMA were assigned computers for work purposes. The employees, including the defendant, were aware as a result of an online training course that by using the computers they consented to the monitoring of any computer activity by the Department of the Interior. In early 2003, the NPS was in the process of upgrading its computers; old computers were stored in the storage area as they were taken out of service. Periodically, an NPS employee, Randall Becker, would take the computers, check them to make sure they did not contain any sensitive or official information on the hard drives, and the NPS would then donate the computers to local schools.

In or around January of 2003, and as this upgrade was occurring, the defendant brought a personal Gateway brand computer from home to work, ostensibly to use it in place of his NPS work computer. When the defendant learned from a superior that he was not permitted to do so, he placed the computer in a bin and placed the bin in the storage area alongside many other

obsolete computers stored there.²

C. On February 6, 2003, a NPS employee found pornography on the defendant's computer.

Weeks later, on February 6, 2003, Randall Becker, a civilian NPS employee, found the Gateway in a container near the other surplus computers. A photograph of the area as it appeared as of February 8, 2003 is attached as Exhibit Two. Thinking it was a government computer, Becker retrieved the Gateway and began looking through the files on the hard drive to assess what treatment the computer needed before it could be donated. In so doing Becker found a file containing many images which appeared to depict child pornography. He also found a picture of a naked man whom he recognized as the defendant.

On February 7, 2003, Becker reported what he had found to his SAMA superiors. They directed Becker to find out who the computer was assigned to and he learned then that the computer did not appear to be registered to anyone working at the SAMA. Later that same day, and in an effort to determine whether the

²The defendant asserts that he placed a note on the computer indicating that it was his. The government expects that the NPS employee who first examined the computer would testify that no such note was on the computer when he found it. As the government argues later, it does not matter whether such a note existed. Among other things, Lewis can be deemed to have abandoned the computer by placing it out of the way with obsolete computers, and his placement of the computer in a common area where all SAMA employees had access to it certainly means that he cannot show an objectively reasonable expectation of privacy in the storage area or the computer itself.

computer was a NPS computer or not, and to whom it belonged if it was, Park Ranger Christopher O'Shea and Special Agent Glenn Van Neil turned the computer on and looked at the same pictures that Becker had seen.

D. On February 8, 2003, the defendant acknowledged the computer was his.

On February 8, 2003, and based on their observations, Ranger O'Shea and SA Van Neil went to the SAMA to meet with Lewis to discuss the images. The meeting, which took place in the Park Rangers' office, was informal, in large part because SA Van Neil and the defendant had known each other for several years, and had even once worked together in New York. After learning why the men were there, the defendant stated that the Gateway computer was his, that he had put it in a bin and placed it in the storage area near several surplus computers after being told he could not use it at work, but that he had placed a sign on it stating "Personal Property Do Not Touch." Lewis acknowledged that he had viewed pornography on the computer via the Internet and was interested in pictures of young boys, but insisted that he had downloaded only pictures where the sites displayed a disclaimer indicating the images were of people over 18 years of age. Lewis denied ever viewing or downloading pornographic material on his government-supplied work computer.

NPS officials subsequently placed the defendant on administrative leave as they investigated the matter further. Lewis returned to work in March of 2003 but resigned his

commission as a law enforcement officer, and took a position as an "interpretation ranger."

E. On June 27, 2003, the defendant consented to a further search of the Gateway computer.

The NPS retained the Gateway computer and the defendant never asked to have it returned. On June 27, 2003, SA's Van Neil and Khela Vasquez met with Lewis to discuss the matter further. SA Vasquez informed Lewis that he was not required to talk to them and that he was free to leave at any time. Lewis reiterated what he had said when first interviewed on February 8, 2003. At the agents' request, Lewis consented to a further search of his personal Gateway computer, and he signed a written consent along with a signed statement attesting to what was said in the meeting.³ A forensic analysis conducted on the computer during summer of 2003 revealed several images of child pornography on the hard drive. The forensic report also showed that the defendant had visited Internet sites entitled "pre-teen, "early

³It is important to clarify an apparent mistaken assumption on the defendant's part. The defendant appears to assert that any consent the government claims he gave the agents on June 27, 2003 was not for any prospective search but, rather, was to apply retroactively to SA Van Neil's search of the defendant's Gateway computer on February 7, 2003, and he devotes considerable energy to arguing why this consent should not be relied upon to justify the earlier search. See Motion at pp. 11-14. To be clear, and as the agents made clear to the defendant, the consent the agents obtained from the defendant on June 27, 2003 was to conduct a **further, future** search of the computer. Accordingly, that section of the defendant's memorandum addressing whether the defendant's consent on June 27, 2003 can be used to support the search on February 7, 2003 is not germane to any issue before the Court and should not be accorded any further attention.

teen," and "lolita," a common name for child pornography on the internet.

F. On February 12, 2004, the defendant consented to a search of his new home computer.

On February 12, 2004, SA Van Neil and Massachusetts State Police Trooper Thomas Neff of the MSP Computer Crimes Unit (Trooper Neff) met with Lewis to discuss the results of the forensic analysis. Prior to meeting with the defendant, SA Van Neil had called and asked the defendant whether the officers could take and search his home computer.⁴ The defendant had agreed to a search but insisted it take place at his residence.

Trooper Neff conducted the search as SA Van Neil and the defendant stood nearby. Trooper Neff found two images that appeared to contain child pornography and two inaccessible files with the titles "lolita" and "pre-teen." Based on the images he observed, and the file names, Trooper Neff concluded that there was probable cause to believe the computer contained contraband and he therefore stopped the search and seized the computer.⁵

G. The defendant called the next day to make a full confession.

On February 13, 2004, the next day, the defendant called SA

⁴To be clear, this home computer was an "E-Mac" brand computer and not the Gateway computer found in the storage area.

⁵Following the search, SA Van Neil realized that, even though he had obtained Lewis's oral consent, he had forgotten to also get written consent, as per his normal practice. So, even though it was not necessary, he asked for and obtained the defendant's written consent to search the computer.

Van Neil at his office and said he wanted to make a statement. On February 16, 2004, SA's Van Neil and Vasquez went to the SAMA to meet with Lewis. They told Lewis that the meeting was in response to his request to SA Van Neil, that he was under no obligation to speak to them, and that he was free to leave at anytime. The defendant then gave a detailed and lengthy statement regarding his use of the computer to collect images depicting child pornography. Among other things, the defendant stated that he had collected images of children as young as 8 years old onto both his old and new computer. He also admitted accessing child pornography on his government computer while on duty as a law enforcement officer. At the conclusion of the meeting, Lewis read and signed a typed statement of the content of the interview.

H. Based on the foregoing, SA Vasquez obtained a warrant to search the computer on March 11, 2004.

On March 11, 2004, and based on all the events from the discovery of pornography on the original Gateway in February of 2003 to Lewis's statement on February 16, 2004, SA Vasquez applied for and obtained a warrant to search the Eachine computer for "images of children engaging in sexually explicit conduct, as defined in 18 U.S.C. section 2256, and files and data related to the knowing receipt and/or possession, in interstate commerce of such images." Addressing the difficulty of conducting forensic analyses, SA Vasquez averred that some computer users try to conceal criminal evidence by storing it in

random order with deceptive file names, so the process of determining which files are evidence of criminal activity can take weeks or months, depending on the volume of data stored.

Following receipt of the warrant, SA Van Neil shipped the computer that day to a forensic analyst with the Department of Interior. On March 16, 2004, the analyst provided a preliminary report indicating that 17 movies saved to the E-Mac's hard drive contained potential child pornography. Upon receiving a hard copy of this report and the accompanying CD-ROM containing the movies on March 24, 2004, SA's Van Neil and Vasquez went to the SAMA to meet with Lewis. Lewis admitted that the material found on the computer was his and he reiterated his previous statements from the February 16, 2004, meeting.

Argument

I. BECKER'S INSPECTION OF THE GATEWAY COMPUTER DID NOT VIOLATE ANY OF THE DEFENDANT'S FOURTH AMENDMENT PROTECTIBLE INTERESTS.

As the party moving for suppression, Lewis bears the burden of establishing that the Fourth Amendment and its protections apply to Becker's inspection of the Gateway. Rakas v. Illinois, 439 U.S. 128, 132 (1979). In so arguing, Lewis contends (or presumes) that Becker's actions amounted to a (1) governmental search which was (2) unreasonable, and which was of an item in which he enjoyed (3) an objectively reasonable expectation of privacy. It did not.

First, there was no governmental search. Becker is a

civilian NPS employee and not a law enforcement officer. No one connected to law enforcement directed Becker to examine the Gateway as opposed to any of the other computers stored in the basement, and no one certainly directed him to look for any contraband. Indeed, Becker was not looking for contraband, but was merely performing his official duties of ensuring computers slated for donation were cleaned before they left the SAMA. Under these circumstances, no governmental search occurred.

Even assuming for the sake of argument that a governmental search occurs whenever anyone hired in any capacity by the state or government inspects an item or place, Becker's conduct was not unreasonable. Again, Becker was not looking for contraband and was merely performing his official duties. It is true that Becker's duty was to inspect surplus NPS computers rather than the defendant's Gateway computer, but Becker believed that the defendant's Gateway computer was a NPS computer. Given that the defendant chose to place the Gateway, of all places at the SAMA, next to the surplus NPS computers, this belief was not only reasonable, but logical and common sensical.

Finally, and for at least two reasons, Lewis cannot meet his burden of showing that he enjoyed an objectively reasonable expectation of the privacy in the Gateway computer. First, by placing the Gateway next to obsolete, government computers slated for donation, and in an area where he had no control over or knowledge of what transpired, Lewis abandoned the Gateway. See

United States v. Austin, 66 F.3d 1115, 1118 (10th Cir. 1995).

The test for abandonment is an objective one that examines the individual's intent, "which may be inferred from words, acts, and other objective facts." United States v. Hernandez, 7 F.3d 944, 947 (10th Cir. 1993). An individual's subjective intent to later retrieve property is alone insufficient to establish that the property was not abandoned. Austin, 66 F.3d at 1118 (although defendant clearly intended to return and retrieve his bag, he had to show more than his subjective intent); United States v. Kendall, 655 F.2d 199, 202 (9th Cir. 1981) (defendant's words and conduct clearly conveyed that he had no expectation of privacy in the bag, even though he fully intended to retrieve it). There is also no evidence that the defendant told anyone at SAMA that he had placed his personal computer in the basement storage area. Even if the defendant were to be heard that he intended to retrieve the Gateway at some later time, his lack of action indicated otherwise, and his subjective intent is irrelevant in any event.

More simply, the defendant cannot demonstrate a reasonable expectation of privacy where he left the computer in a common area of the building where up to 40 employees had the right to be at any given time. There were no cubicles or partitions distinctively separating the computers from each other or the rest of the storage area. Accordingly, where defendants place items in a common area where they expose them to the public and

run the risk that a third party might take or search the item, courts have repeatedly refused to find a reasonable expectation of privacy. United States v. Hawkins, 139 F.3d 29, 32 (1st Cir. 1998) (no reasonable expectation of privacy in unenclosed area of the basement in apartment building); United States v. Thornley, 707 F.2d 622, 624-625 (1st Cir. 1983) (defendant had no reasonable expectation of privacy in basement storage area because the door was not kept locked and access was not restricted to any of the tenants).

II. LEWIS'S STATEMENTS ON FEBRUARY 8, 2003, JUNE 27, 2003, FEBRUARY 16, AND MARCH 24, 2004 WERE VOLUNTARY.

Devoting little more than three paragraphs to the claim, the defendant argues that the statements he made to officers and agents on various occasions should be suppressed because the agents effectively coerced the statements from him, rendering them involuntary. Motion at pp. 15-16. This claim is wholly without merit.

Whether an admission was made voluntarily without coercion is to be decided in light of the totality of the circumstances. United States v. Jackson, 918 F.2d 236, 241 (1st Cir. 1990). There is simply no evidence to suggest that any of the statements the defendant made were coerced or involuntary. On the contrary, Lewis was a law enforcement officer who was made aware at the beginning of each meeting what its purpose was. He also understood, both by virtue of his professional training and experience and what agents told him, that he was not in custody,

did not have to say anything, and could leave at any time. The interview on February 8, 2003, took place in Lewis's own office, and he was allowed to keep his gun and sit wherever he wanted. Before the June 27, 2003, meeting, Agent Vasquez specifically told Lewis that any statements he made were voluntary and that he was free to leave at any time, and Lewis signed a statement to that effect. Additionally, at both the June 27, 2003 meeting and the February 12, 2004 meeting, Lewis signed forms saying that he voluntarily gave consent for the search of the Gateway and the E-Mac computer at his home, respectively, and Lewis contacted the agents on his own following the February 12th search to express his willingness to make a full statement. Considering the totality of the circumstances, Lewis voluntarily participated in any and all interviews after the Gateway was seized and the contents of these interviews are admissible.

III. THE AGENTS HAD PROBABLE CAUSE TO SEIZE THE E-MAC COMPUTER FOLLOWING TROOPER NEFF'S DISCOVERY OF PORNOGRAPHY ON IT.

During his manual search of the E-Mac computer, Trooper Neff found several images of what he believed to be child pornography as well as inaccessible files entitled "lolita" and "pre-teen." Trooper Neff's findings were sufficient to establish probable cause; consequently, the seizure of the E-Mac was lawful. "The touchstone of the Fourth Amendment is reasonableness," Jimeno, 500 U.S. at 250, and as such, it "does not require officers to be correct in their assessment of facts; it requires them only to be reasonable." United States v. Marshall, 348 F.3d 281, 288 (1st

Cir. 2003). Trooper Neff and Agent Van Neil believed that the images on the E-Mac were of child pornography and they based this belief on their own experience, the knowledge that Lewis possessed child pornography on the Gateway, and the similar file names on both the Gateway and the E-Mac computers. Because Trooper Neff and SA Van Neil had a reasonable belief that the images they found depicted child pornography, the seizure of the E-Mac was lawful.⁶

IV. THE WARRANT TO SEARCH THE E-MAC WAS VALID AND THE SEARCH COMMENCED WITHIN THE TIME PERIOD ALLOWED BY THE WARRANT.

On March 11, 2004, Agent Vasquez applied for a search warrant to search the E-Mac computer for pornographic images containing children. In her affidavit supporting the application, Agent Vasquez included information about the initial search and seizure of the Gateway, the images of child

⁶The defendant contends that every search, seizure and interview following Becker's initial foray into the Gateway computer must be suppressed as fruit of the poisonous tree in light of Wong Sun v. United States, 371 U.S. 471 (1963). However, these claims, rarely asserted with any force, fail easily because the agents' conduct was proper and lawful. Moreover, Lewis's consent to each interview and to all but the last search cured any illegality assuming there was any. The test for whether evidence should be excluded as the fruit of the poisonous tree is "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." Wong Sun v. United States, 371, U.S. 471, 488 (1963). It is well established that voluntary consent is sufficient to purge the taint of any potential illegalities. See, e.g., United States v. Race, 529 F.2d 12, 15 (1st Cir. 1976). By consenting to the searches and interviews, and even contacting the agents to speak to them on one occasion, Lewis surely purged the taint of any illegal conduct.

pornography found on the Gateway, the statements made by Lewis on February 8, 2003 and June 27, 2003, the search and subsequent seizure of the E-Mac, and the inculpatory statements made by Lewis on February 16, 2004. After the warrant was issued on March 11, 2004, Agent Vasquez immediately began execution of the warrant by sending the E-Mac to the Department of Interior in Denver, CO for forensic analysis that same day. Because the warrant and its supporting affidavit were sufficiently specific as to what was to be searched and the time frame required for the search, the warrant to search the E-Mac is valid and the evidence recovered from the search is admissible.

The Fourth Amendment requires a warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. A warrant must describe "the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings," United States v. Carey, 172 F.3d 1268, 1271 (10th Cir. 1999), and the particularity requirement is satisfied if the warrant would permit an executing officer to reasonably know what items are to be searched. United States v. Layne, 43 F.3d 127, 132 (5th Cir. 1995). Warrants rarely prescribe the method or procedure necessary to perform a search because "the warrant process is primarily concerned with identifying *what* may be searched or seized-not how-and *whether* there is sufficient cause for the invasion of privacy thus entailed. United States v. Upham, 168

F.3d 532,537 (1st Cir. 1999) (emphasis in original).

The warrant to search the E-Mac did not authorize a general search of the computer; rather, it was sufficiently particular as to what was to be searched. It indicated that the computer was to be searched for "images of children engaging in sexually explicit conduct," and this description adequately limited the search to only those particular images. A number of courts have upheld warrants similar to the one here as being sufficiently particular as to what was to be searched. United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (warrant was directed at items relating to child pornography and did not authorize a general inspection of defendant's residence); United States v. Hall, 142 F.3d 988, 996-997 (7th Cir. 1998) ("items listed on the warrants were qualified by phrases that emphasized that the items sought were those related to child pornography"). Because the warrant was particular as to the images to be searched, the fact that it did not specify a particular method for limiting the search to only those images does not render the warrant invalid.

Lewis further argues that the search of the E-Mac was invalid because the entire forensic search was not completed before the warrant's March 21, 2004 expiration date. This argument fails, however, because the warrant did not require that the agents complete the complex forensic analysis of the E-Mac by March 21, 2004. Rather it required only that the agents begin

the execution of the search within that 10 day time period.

Because the agents began the search process immediately after the warrant was issued, the search of the E-Mac was timely and the evidence gathered from the forensic search is admissible.

The Federal Rules of Criminal Procedure requires that a warrant must "command the officer to *execute* the warrant within a specified time no longer than 10 days." Fed. R. Crim. P. 41(e)(2)(A)(emphasis added). The Fourth Amendment does not specify the duration of a warrant or when a search or seizure must occur, but the Federal Rules require that the warrant expire within 10 days to ensure that probable cause to search continues to exist. See United States v. Gerber, 994 F.2d 1556, 1559-1560 (11th Cir. 1993). Here, the search was executed within the 10 days specified in the warrant and probable cause to perform the search did not dissipate; thus, the search of the E-Mac was timely.

As stated above, Agent Van Neil sent the E-Mac computer to Denver, CO for forensic analysis the same day the warrant was issued. A preliminary analysis was then immediately performed and the report regarding this analysis was received by Van Neil on March 16, 2004, five days before the warrant was to expire on March 21, 2004. It is unreasonable to expect a complex forensic search of a computer to be completed in only 10 days, and the fact that a preliminary search was completed before the warrant's expiration date is sufficient "execution" as required by the

Federal Rules of Criminal Procedure. Additionally, the images and data contained in the E-Mac did not change upon the expiration of the warrant on March 21, 2004, and the preliminary analysis of the E-Mac revealed several movies which appeared to contain child pornography, so probable cause to search the E-Mac clearly continued to exist 10 days after the warrant was issued. Finally, in her affidavit supporting the warrant application, Agent Vasquez specifically stated that searching and analyzing computers is a highly technical process that can often take weeks or months. Even Magistrate Dein, in authorizing the warrant, recognized that the complete forensic analysis of the E-Mac would not be completed before the warrant's March 21, 2004 expiration date. The search of the E-Mac began within the time period specified by the warrant and the entire forensic analysis was completed within a reasonable time, so the evidence recovered from the E-Mac is admissible.

Conclusion

For the reasons set forth above, the United States respectfully requests that the Court deny the defendant's Motion.

Respectfully submitted,

MICHAEL J. SULLIVAN
United States Attorney

By:

/s/Donald L. Cabell
DONALD L. CABELL
Assistant U.S. Attorney